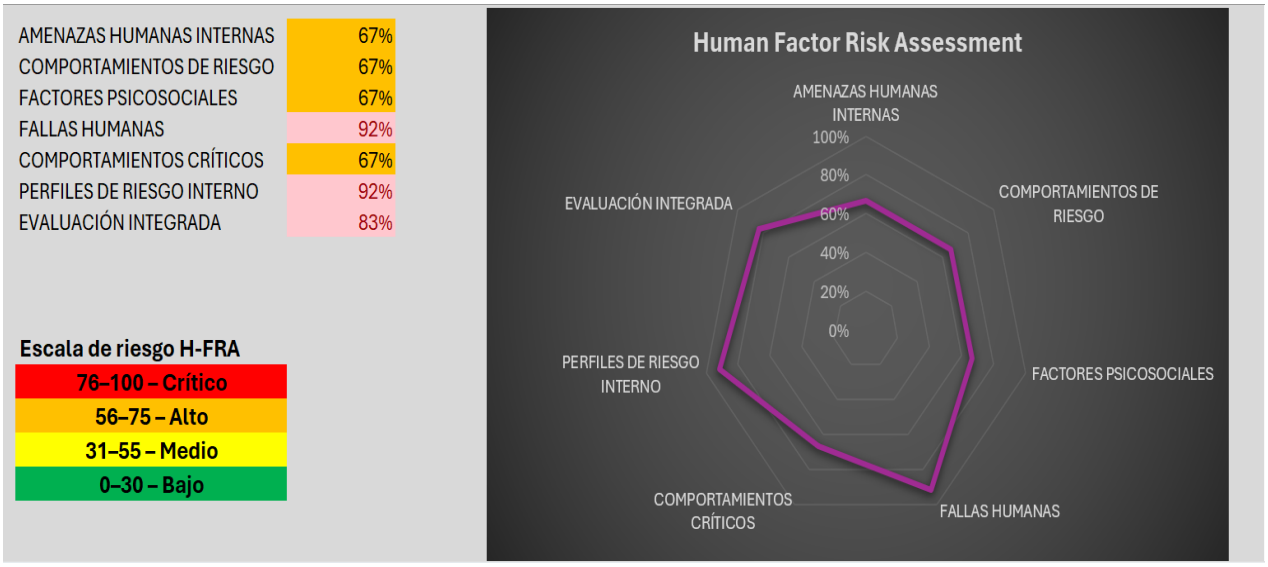
Manual Integral de Análisis de Riesgo Basado en Factor Humano (H-FRA)

Smart Prevention Through Human Factor Risk Analysis



Autor: Mauricio Alan Illera Díaz

ORCID ID: 0009-0001-1505-4170

Researcher ID: OSI-4768-2025

Licencia: Creative Commons BY-NC-SA 4.0

Declaración de Principios

La organización adopta el presente Protocolo Integral H-FRA con el propósito de prevenir, detectar y mitigar riesgos derivados del comportamiento humano que puedan comprometer activos, información, operaciones o la continuidad del negocio. Este sistema se sustenta en tres principios rectores que garantizan su legitimidad, coherencia técnica y respeto ético:

Prevención Proactiva

La organización se compromete a anticipar los riesgos antes de que se materialicen en incidentes, pérdidas o afectaciones operativas.
El enfoque es predictivo y preventivo, no reactivo, priorizando la identificación temprana de conductas, patrones y factores que puedan aumentar la probabilidad de un evento no deseado.

Método Sistemático y Replicable

Todas las actividades del modelo H-FRA deben ejecutarse mediante procedimientos estandarizados, verificables y repetibles.
Esto asegura:

consistencia metodológica entre áreas y evaluadores,

trazabilidad documental,

resultados comparables a lo largo del tiempo, y

una evaluación justa basada en criterios y evidencias objetivas.

La uniformidad del proceso es esencial para la confiabilidad del sistema.

Respeto Absoluto a la Dignidad Humana

El modelo H-FRA se fundamenta en el respeto integral al colaborador.
El análisis se centra exclusivamente en conductas, accesos, factores de riesgo y evidencia verificable, nunca en características personales, creencias, preferencias o elementos de la vida privada.

La organización garantiza: ausencia total de discriminación, confidencialidad en el manejo de datos, ética en la observación e interacción, y protección de los derechos laborales.

Ninguna evaluación puede utilizarse como herramienta de persecución o castigo sin sustento.

1. Introducción

El protocolo H-FRA integra metodologías provenientes de la seguridad industrial, aviación, psicología laboral y seguridad corporativa. Su finalidad es evaluar el riesgo generado por el factor humano, orientándose a la prevención de robo interno, fuga de información, sabotaje, fraude y fallas humanas. Para ello, se realiza un análisis estructurado de conductas, accesos, motivaciones y condiciones psicosociales.

2. Métodos de Análisis de Riesgo Basados en Comportamiento Humano

2.1 Human Factors Analysis and Classification System (HFACS)

El sistema HFACS permite evaluar diversos aspectos que influyen en la ocurrencia de incidentes derivados del factor humano. Se examinan errores, violaciones, fatiga, fallas cognitivas, problemas de comunicación y aspectos relacionados con la cultura organizacional. Este método clasifica las fallas humanas en varios niveles: actos inseguros cometidos por las personas, precondiciones que pueden propiciar dichos actos, supervisión deficiente y factores organizacionales que impactan el comportamiento de los colaboradores.

2.2 Human Reliability Analysis (HRA)

El análisis HRA utiliza técnicas como THERP y HEART para estimar la probabilidad de error humano en distintas tareas. Este enfoque permite identificar cuáles tareas son críticas y requieren mayor atención, así como establecer contramedidas específicas. Entre estas acciones se incluyen el fortalecimiento del entrenamiento, el rediseño de tareas para reducir riesgos y la automatización controlada de procesos cuando sea pertinente.

2.3 Behavior-Based Safety (BBS)

La metodología BBS se enfoca en la observación de conductas de los colaboradores para prevenir incidentes. Mediante este método se distinguen hábitos de riesgo, distracciones y desviaciones de los procedimientos establecidos, promoviendo el uso de refuerzos positivos y la aplicación de correcciones en tiempo real para reducir la probabilidad de accidentes.

2.4 Análisis Psicosocial del Riesgo Laboral

Este análisis contempla la evaluación de factores como el estrés, la carga laboral, el clima organizacional, las emociones y la fatiga. Reconoce la influencia directa que estos elementos tienen en el aumento de la probabilidad de errores o en la aparición de conductas inapropiadas dentro de la organización.

2.5 Insider Threat Risk Assessment

El modelo de evaluación de amenazas internas se emplea en el ámbito de la seguridad corporativa para identificar riesgos relacionados con la intención de los colaboradores. Considera situaciones de descontento, sabotaje, fraude, fuga de datos y abuso de privilegios, permitiendo anticipar posibles incidentes intencionados que puedan afectar a la organización.

2.6 Modelos de Comportamiento en Seguridad Física

Estos modelos se utilizan para analizar acciones que pueden facilitar el robo interno o la ocurrencia de pérdidas. Se estudian rutinas inseguras, accesos no autorizados, manipulación irregular y negligencias, con el objetivo de detectar conductas que representen un riesgo para la seguridad física de la empresa.

3. Análisis de Riesgo Humano para Prevención de Robo y Fuga

El análisis de riesgo humano dirigido a la prevención de robo y fuga dentro de la organización implica una revisión exhaustiva de las posibles amenazas internas. Este proceso abarca la identificación de actores que pueden tener intenciones maliciosas, aquellos que actúan de manera negligente o casos donde ambos perfiles se combinan. Para lograrlo, se estudian patrones de conducta observados entre los colaboradores, así como se monitorean indicadores financieros que pueden señalar situaciones anómalas, tales como cambios repentinos en el comportamiento económico o señales de estrés financiero.

Asimismo, se presta especial atención a la detección de señales de deterioro emocional entre los empleados, ya que estas pueden ser precursoras de incidentes de seguridad. El propósito central de este análisis es anticipar la ocurrencia de eventos indeseados, permitiendo así la activación oportuna de medidas preventivas que salvaguarden los activos y la información de la organización.

4. Factores Psicosociales que Incrementan el Riesgo

Diversos factores psicosociales presentes en el entorno laboral pueden incrementar de manera significativa el riesgo de errores o conductas desleales por parte de los colaboradores. Entre estos factores se encuentran los turnos de trabajo extensos, los cuales pueden generar fatiga y disminuir los niveles de atención de los empleados.

Un clima organizacional tóxico, caracterizado por relaciones laborales problemáticas o falta de apoyo, también puede favorecer la aparición de comportamientos no deseados. De igual manera, la existencia de políticas ambiguas, la comunicación deficiente entre los

diferentes niveles de la organización y la asignación de cargas de trabajo excesivas contribuyen a un entorno propenso a la comisión de errores o a la adopción de actitudes desleales.

5. Análisis de Fallas Humanas (HFACS – THERP – HEART)

El análisis integra metodologías reconocidas para identificar y comprender errores humanos que pueden originar incidentes operativos o de seguridad. Se consideran:

Errores de omisión: pasos no realizados o actividades incompletas.

Errores de comisión: acciones incorrectas, fuera de secuencia o inapropiadas.

Violaciones: incumplimientos deliberados de normas, procedimientos o controles establecidos.

Decisiones inadecuadas: elecciones mal fundamentadas derivadas de información insuficiente o interpretación deficiente.

Factores contribuyentes: fatiga, sobrecarga de trabajo, condiciones ergonómicas deficientes, entrenamiento insuficiente, presión operativa, entre otros.

Este análisis permite determinar causas raíz asociadas al factor humano y diseñar medidas de mitigación orientadas a mejorar desempeño, reducir la probabilidad de error y fortalecer la cultura de seguridad.

6. Análisis Conductual (BBS-H)

El enfoque de Seguridad Basada en el Comportamiento (Behavior-Based Safety for Humans) se utiliza para observar y evaluar conductas críticas que puedan representar un riesgo para la organización. Las observaciones se aplican en:

Seguridad física del personal.

Protección de activos e infraestructura.

Control de accesos y cumplimiento de protocolos.

Resguardo, manejo y confidencialidad de la información.

El objetivo es identificar patrones conductuales inseguros, reforzar prácticas adecuadas y desarrollar intervenciones que promuevan comportamientos seguros y consistentes.

7. Perfiles de Riesgo Interno

La identificación de perfiles de riesgo interno permite anticipar conductas que podrían comprometer la seguridad operativa, la integridad de la información y la protección de activos. Entre los perfiles más relevantes se consideran:

Descontento / Vengativo:
Individuos con insatisfacción marcada, percepción de injusticia o conflicto con la organización, lo que puede derivar en acciones intencionales de daño, sabotaje o filtración de información.

Oportunista:
Personas que aprovechan brechas de control o situaciones favorables para obtener beneficios personales, ya sea mediante abuso de privilegios, fraude o uso indebido de recursos.

Negligente Crónico:
Colaboradores con patrones persistentes de incumplimiento, descuido o falta de apego a procedimientos, aumentando la probabilidad de errores operativos, incidentes y vulneraciones.

Colaborador Externo:
Actores ajenos a la organización que, mediante manipulación, coerción o relación con personal interno, buscan obtener acceso a información o activos a través del aprovechamiento de debilidades humanas.

Estrés Financiero:
Situación personal que puede incrementar el riesgo de comportamientos indebidos, como fraude, mal uso de recursos o colaboración con terceros, especialmente cuando se combina con altos niveles de presión o acceso privilegiado.

8. Modelo Integrado H-FRA – 7 Dimensiones

El modelo H-FRA (Human Factor Risk Assessment) integra diferentes variables del factor humano para evaluar el riesgo asociado a individuos, roles o situaciones específicas dentro de la organización. El análisis se estructura en siete dimensiones clave:

D1. Intención:
Evalúa el propósito o motivación detrás de una acción, ya sea positiva, neutral o potencialmente dañina. Permite distinguir entre errores involuntarios y conductas deliberadas.

D2. Conducta Observable:
Analiza comportamientos visibles y medibles, facilitando la identificación de desviaciones, patrones de riesgo y señales tempranas de incidentes.

D3. Estado Psicosocial:
Considera condiciones personales, emocionales y sociales que pueden influir en el desempeño y la toma de decisiones, como estrés, presión laboral, conflictos o desgaste.

D4. Fallas Humanas:
Integra errores de omisión, comisión, violaciones y decisiones inadecuadas, así como factores contribuyentes como fatiga, mala ergonomía o entrenamiento insuficiente.

D5. Conductas Críticas:
Identifica comportamientos que representan un riesgo directo para la seguridad, la continuidad operativa o la protección de activos, alineándose con metodologías BBS-H.

D6. Perfil Interno:
Clasifica características individuales y patrones conductuales en perfiles de riesgo (oportunista, negligente, descontento, etc.) que ayudan a anticipar vulnerabilidades.

D7. Evaluación Integrada (Probabilidad × Motivación × Acceso × Impacto):
Combina los factores anteriores en un índice de riesgo cuantificado, considerando la probabilidad del evento, el nivel de motivación, el acceso disponible y el potencial impacto para la organización.

9. Sistema de Puntaje H-FRA

El rango va de 0 a 100 e incluye variables como conducta, accesos, motivación psicosocial, historial, exposición a tentaciones y obediencia a políticas. El puntaje permite clasificar el nivel de riesgo y definir las acciones correspondientes.

11. Ciclo de Evaluación H-FRA

El ciclo de evaluación H-FRA establece un proceso sistemático para identificar, analizar y gestionar riesgos asociados al factor humano dentro de la organización. Sus etapas son:

Filtro:
Selección inicial de casos, situaciones o individuos que requieren análisis, basada en alertas, indicadores o criterios predefinidos.

Recolección:
Obtención de información relevante mediante registros, reportes operativos, datos de desempeño, antecedentes y fuentes documentales.

Observación:
Evaluación directa de comportamientos, interacciones y prácticas en el entorno real, identificando patrones o desviaciones.

Entrevista:
Profundización cualitativa para comprender contexto, motivaciones, percepciones y factores psicosociales que influyen en la conducta.

Matriz:
Integración estructurada de la información en una matriz analítica que organiza hallazgos por dimensiones del modelo H-FRA.

Puntaje:
Asignación de valores cuantitativos mediante criterios estandarizados, obteniendo un nivel de riesgo calculado.

Decisión:
Determinación del curso de acción a partir del puntaje y del análisis integral: mitigación, intervención, monitoreo o cierre.

Plan:
Diseño de un plan de acción que incluye medidas preventivas, correctivas o formativas, responsables y plazos.

Seguimiento:
Monitoreo continuo del cumplimiento del plan, evolución del riesgo y cambios en el comportamiento o condiciones.

Cierre:
Conclusión formal del caso o evaluación, documentando resultados, lecciones aprendidas y recomendaciones para futuros ciclos.

12. Objetivo y Alcance

El objetivo del protocolo es establecer un sistema único y repetible para identificar, cuantificar y mitigar riesgos humanos antes de que se conviertan en pérdidas. El alcance abarca a todo el personal y activos de la organización, incluyendo empleados, contratistas, terceros y ex-empleados con accesos residuales.

13. Responsabilidades y Roles

Las responsabilidades se distribuyen entre la Dirección de Seguridad Corporativa, el equipo H-FRA (psicología laboral, RRHH, TI, supervisores) y el Comité de Escalamiento, que incluye representantes de DSC, RRHH, Legal y Gerencia General.

14. Frecuencia de Aplicación

Alta criticidad: cada 6 meses

Media criticidad: cada 12 meses

Baja criticidad: cada 24 meses

Aplicación por eventos: incidentes, fusiones, denuncias, cambios organizativos

15. Requisitos Previos

Para la implementación efectiva del modelo H-FRA y sus procesos asociados, la organización debe contar con los siguientes requisitos fundamentales:

Política de Cero Tolerancia:
Lineamientos institucionales que establecen límites claros frente a conductas indebidas, violaciones de seguridad y actos que comprometan la integridad operativa o ética.

Inventario Dinámico de Accesos:
Registro actualizado y automatizado de permisos, privilegios y accesos a sistemas, instalaciones y activos. Debe reflejar cambios en roles, rotaciones y necesidades operativas en tiempo real.

Base de Datos Unificada (sin información personal sensible):
Plataforma centralizada para almacenar indicadores, observaciones y resultados del modelo H-FRA, garantizando la protección de la privacidad y cumpliendo estándares de minimización de datos.

Capacitación Anual Obligatoria:
Programa de formación continua que refuerce competencias en seguridad, conducta responsable, factor humano y cumplimiento normativo, asegurando una actualización periódica del personal.

16. Flujo de Trabajo H-FRA – Paso a Paso

El flujo de trabajo H-FRA establece una secuencia operativa estandarizada para evaluar el riesgo asociado al factor humano y aplicar acciones correctivas o preventivas de manera oportuna. El proceso comprende:

Pre-filtro:
Identificación inicial de casos mediante alertas, indicadores o criterios definidos, determinando si requieren un análisis formal.

Recolección de Datos:
Compilación de información relevante proveniente de registros operativos, accesos, desempeño, antecedentes y fuentes internas autorizadas.

Observaciones en Tres Momentos:
Evaluación conductual en distintos contextos o momentos operativos para asegurar una visión objetiva, estable y consistente del comportamiento.

Entrevista de 25 Minutos:
Conversación estructurada para explorar percepciones, motivaciones, factores psicosociales y contexto laboral, complementando la información observada.

Cruce de Accesos:
Validación de los privilegios, accesos físicos y lógicos del individuo, contrastándolos con su rol, actividades observadas y requerimientos operativos.

Cálculo de Puntaje:
Evaluación cuantitativa basada en el modelo H-FRA, incorporando probabilidad, motivación, acceso e impacto para obtener un nivel de riesgo integral.

Clasificación:
Asignación del caso a una categoría de riesgo (bajo, medio, alto o crítico), orientando la toma de decisiones.

Diseño del Plan de Tratamiento:
Definición de medidas preventivas o correctivas, capacitación, restricciones de acceso, acompañamiento, o acciones disciplinarias según corresponda.

Seguimiento:
Monitoreo sistemático de la evolución del caso, verificación del cumplimiento del plan y ajustes necesarios.

Cierre Documental:
Finalización formal del proceso, archivando resultados, decisiones y lecciones aprendidas, asegurando trazabilidad y mejora continua.

17. Criterios de Evaluación Conductual (BBS-H)

Los criterios BBS-H se enfocan en la observación directa de comportamientos que impactan la seguridad física, la protección de información y la integridad operativa. Cada conducta se evalúa bajo los principios de observación objetiva, no punitiva y orientada a la mejora.

17.1 Observación de Puertas de Seguridad

Revisión del uso correcto de credenciales, cierre total de puertas, ausencia de “tailgating” y respeto de zonas restringidas.

17.2 Uso de Dispositivos USB

Verificación de que únicamente se utilicen dispositivos corporativos autorizados, etiquetados y registrados. Cualquier uso no justificado se considera desviación.

17.3 Impresión de Documentos Sensibles

Confirmación de que los documentos clasificados se retiren inmediatamente de la impresora, evitando exposición o abandono en áreas comunes.

17.4 Limpieza de Escritorio (“Clean Desk”)

Evaluación del cumplimiento de la política de orden y resguardo: no dejar contraseñas, archivos sensibles o dispositivos sin supervisión.

17.5 Firma y Autorización de Documentos

Revisión del proceso de validación previa a la firma, especialmente cuando el monto o impacto supera límites definidos por finanzas o el área responsable.

17.6 Cumplimiento General de Protocolos

Comprobación del respeto a procedimientos operativos, normas de acceso, manejo de información, uso de EPP (si aplica) y cumplimiento documental.

Clasificación de la Observación

Cada conducta observada se registra bajo uno de los siguientes niveles:

Correcto: Cumplimiento pleno del estándar sin riesgo asociado.

Desviación Leve: Incumplimiento menor sin impacto inmediato, pero que incrementa la probabilidad futura de riesgo.

Desviación Crítica: Comportamiento que compromete directamente la seguridad, protección de activos o confidencialidad, requiriendo acción inmediata.

18. Indicadores de Alerta Temprana (EWI)

Los Early Warning Indicators (EWI) permiten detectar señales tempranas de riesgo derivadas del comportamiento humano antes de que se materialicen incidentes de robo interno, fuga de información o sabotaje. Su función es activar intervenciones preventivas basadas en evidencia.

18.1 Indicadores Técnicos

Relacionados con el uso de sistemas, accesos lógicos y actividad digital.

Descarga masiva no justificada: volúmenes atípicos de archivos o información en un periodo corto.

Accesos fuera de horario: ingresos al sistema o áreas restringidas sin ticket, autorización o motivo operacional.

Intentos fallidos de autenticación: múltiples intentos fallidos que sugieren prueba de contraseñas, descuido o actividad sospechosa.

Uso no autorizado de USB o almacenamiento externo (si aplica).

Modificación o borrado inesperado de archivos sensibles.

18.2 Indicadores Conductuales

Derivados de la observación diaria y cambios comportamentales abruptos.

Cambios bruscos en horarios de entrada y salida (variaciones superiores a 60 minutos sin justificación).

Resistencia persistente a tomar vacaciones, rotar turnos o delegar tareas críticas.

Incremento significativo de quejas, conflictos o fricciones con el equipo o supervisores.

Aislamiento repentino, pérdida de interés o cambios notables en el estado de ánimo.

Desviaciones frecuentes a protocolos o controles internos.

18.3 Indicadores Financieros y Personales

Señales que pueden incrementar la vulnerabilidad a conductas oportunistas o a coacción externa.

Solicitudes recurrentes de adelantos salariales más allá del comportamiento habitual.

Embargos, deudas formales o notificaciones judiciales informadas a RRHH.

Cambios en el estilo de vida no acordes al nivel de ingresos, cuando sean evidentes y manifiestos.

Comentarios sobre dificultades económicas que afecten el desempeño o estabilidad emocional.

18.4 Activación de Alertas

El sistema establece umbrales de activación para permitir respuestas oportunas:

Alerta Amarilla:
Se activa cuando se presentan:

Dos (2) indicadores técnicos, o

Dos (2) indicadores conductuales, o

Un técnico + un conductual de alto impacto.

La Alerta Amarilla conduce a una entrevista inmediata, revisión de accesos, y pre-evaluación H-FRA según el protocolo.

19. Mitigaciones por Perfil de Riesgo Interno

Las estrategias de mitigación se diseñan según el tipo de perfil identificado en el análisis H-FRA. Cada intervención busca reducir la probabilidad de ocurrencia, controlar los accesos, estabilizar factores psicosociales y corregir desviaciones conductuales antes de que evolucionen hacia un incidente crítico.

19.1 Perfil Descontento – Vengativo

Objetivo: reducir la motivación negativa, restablecer la percepción de justicia y evitar conductas retaliatorias.

Medidas de mitigación:

Reasignación temporal o permanente de área para disminuir tensiones.

Cambio de supervisor directo cuando existan indicadores de conflicto persistente.

Programas de escucha activa y mediación laboral.

Intervención de clima organizacional si el conflicto es colectivo.

Seguimiento quincenal durante los primeros 90 días.

19.2 Perfil Oportunista

Objetivo: disminuir la posibilidad de explotación de vulnerabilidades operativas y cerrar brechas en controles internos.

Medidas de mitigación:

Separación de funciones (SoD) en tareas críticas.

Implementación de doble autorización para operaciones sensibles.

Rotación obligatoria de puesto o funciones cada 6 meses en áreas de riesgo.

Revisión mensual de accesos lógicos y físicos.

Incremento de trazabilidad mediante logs ampliados o revisiones periódicas.

19.3 Perfil Negligente Crónico

Objetivo: corregir hábitos inseguros o desviaciones recurrentes que incrementan la probabilidad de fallas humanas.

Medidas de mitigación:

Re-entrenamiento práctico mediante sesiones uno a uno.

Refuerzo visual de procedimientos (señalización, recordatorios, guías rápidas).

Auditorías sorpresa mensuales para validar mejora conductual.

Mentoría con supervisores para reforzar disciplina operativa.

Revisión del diseño de tareas para descartar sobrecarga o mala ergonomía.

19.4 Perfil Colaborador Externo

Objetivo: evitar infiltración, fuga de información o uso indebido de accesos por parte de terceros vinculados al empleado.

Medidas de mitigación:

Addendum reforzado de confidencialidad o cláusulas restrictivas.

Limitación estricta de acceso físico, lógico y horario.

Revisión de mochilas o bienes al ingresar y salir (según marco legal).

Supervisión reforzada en áreas sensibles.

Registro detallado de visitantes, proveedores y contratistas vinculados.

19.5 Perfil con Estrés Financiero

Objetivo: reducir la vulnerabilidad a la coacción, fraude o robo motivado por necesidad económica.

Medidas de mitigación:

Asesoría financiera confidencial y sin costo.

Acompañamiento psicológico para manejo de estrés y toma de decisiones.

Canalización a programas internos de apoyo (si existen).

Pago de nómina exclusivamente por cuentas bancarias reguladas, evitando prácticas informales.

Seguimiento trimestral para evaluar estabilidad financiera y emocional.

20. Documentos Obligatorios del Sistema H-FRA

El proceso H-FRA requiere la generación, resguardo y trazabilidad de documentación formal que respalde cada etapa del análisis, las decisiones tomadas y las acciones implementadas. Todos los documentos deben gestionarse conforme a las políticas de confidencialidad, conservación y acceso seguro de la organización.

20.1 Ficha Individual H-FRA

Documento base que consolida la información del caso evaluado.
Incluye:

Datos laborales no sensibles

Resultados de observación BBS-H

Indicadores EWI detectados

Accesos físicos y lógicos relevantes

Puntaje H-FRA y categoría de riesgo

Línea del tiempo del caso

20.2 Acta de Entrevista Semiestructurada

Registro formal de la sesión de entrevista.
Debe contener:

Fecha, lugar y duración

Temas evaluados y hallazgos

Resumen de percepciones psicosociales

Firma del entrevistador y del colaborador (o constancia de negativa)

20.3 Plan de Tratamiento del Riesgo

Documento que define las acciones preventivas o correctivas asociadas al caso.
Incluye:

Acciones a implementar (máx. 3 correctivas y 2 preventivas)

Responsable asignado

Fechas compromiso y criterios de éxito

Evidencias de cumplimiento

Resultados de seguimiento a 30, 90 y 180 días

20.4 Alerta Temprana (EWI)

Reporte que se genera ante la activación de una Alerta Amarilla.
Debe contemplar:

Indicadores que activaron la alerta

Evaluación preliminar del riesgo

Acciones inmediatas tomadas

Recomendación de apertura o no de un caso formal H-FRA

20.5 Reporte Anual Consolidado

Documento corporativo que recopila todas las tendencias del año.
Debe incluir:

Estadísticas por área, puesto, antigüedad y categoría de riesgo

Incidentes evitados o mitigados

Evolución de puntajes y recurrencia de hallazgos

Eficacia del programa H-FRA

Recomendaciones de mejora para el siguiente ciclo

21.1 Cobertura

Definición:
Porcentaje de personal evaluado respecto al personal planificado en cada ciclo.

Objetivo:
Asegurar que la aplicación del modelo alcance a la totalidad de los grupos definidos por nivel de criticidad.

Indicadores sugeridos:

% de cumplimiento del plan anual

% de áreas evaluadas vs. áreas programadas

21.2 Eficiencia

Definición:
Tiempo promedio entre la apertura del caso y su cierre documental.

Objetivo:
Reducir los tiempos del ciclo, optimizar recursos y evitar retrasos que permitan la evolución del riesgo.

Indicadores sugeridos:

Días promedio de resolución

% de casos que exceden el tiempo estándar establecido

21.3 Eficacia

Definición:
Grado de reducción del riesgo interno tras aplicar el plan de tratamiento.

Objetivo:
Medir la capacidad del programa para disminuir el H-FRA Score en la población evaluada.

Indicadores sugeridos:

Diferencia del H-FRA Score antes y después de la intervención

% de reincidencia de desviaciones conductuales

% de cumplimiento de acciones correctivas

21.4 Retorno de la Inversión (ROI) Estimado

Definición:
Relación entre los costos del programa H-FRA y el valor económico de incidentes internos evitados o mitigados.

Objetivo:
Demostrar el impacto financiero del modelo y justificar su continuidad o ampliación.

Fórmula recomendada:

ROI = (Costo promedio de incidente interno × Número de incidentes evitados) – Costo total del programa H-FRA

Indicadores sugeridos:

Ahorro anual proyectado

Comparativo año contra año

% de reducción en incidentes de seguridad interna

22. Revisión y Mejora Continua

El sistema H-FRA se basa en un ciclo permanente de actualización que garantiza su vigencia, precisión y alineación con prácticas internacionales de gestión del riesgo humano. La revisión continua permite adaptar el modelo a cambios operativos, regulatorios y contextuales de la organización.

22.1 Revisión Anual del Protocolo

Cada 12 meses, la Dirección de Seguridad Corporativa realiza una revisión integral del protocolo, evaluando:

Coherencia del modelo con los riesgos actuales de la organización.

Eficacia de los criterios de evaluación conductual, psicosocial y técnico-digital.

Desempeño de las métricas de gestión (cobertura, eficiencia, eficacia, ROI).

Calidad de la documentación generada y cumplimiento del ciclo H-FRA.

Necesidad de actualizar procedimientos, plantillas o herramientas.

La revisión debe quedar documentada y aprobada por el Comité de Riesgos.

22.2 Incorporación de Nuevos Indicadores EWI

El sistema se actualiza con nuevos indicadores de alerta temprana provenientes de:

Threat intelligence interno o externo.

Incidentes recientes, aprendizajes y lecciones identificadas.

Cambios en patrones de fraude, fuga de información o robo interno.

Recomendaciones de auditoría interna o externa.

Los indicadores obsoletos se sustituyen o ajustan para mejorar la capacidad predictiva del modelo.

22.3 Alineación con Auditorías Externas y Normas Internacionales

La mejora continua considera los hallazgos provenientes de auditorías certificadas y marcos de referencia como:

ISO 27001 (Seguridad de la Información)

ISO 31000 (Gestión del Riesgo)

ISO 45001 (Seguridad y Salud en el Trabajo)

Modelos HRA, HFACS y BBS internacionales

Buenas prácticas de NIST y organismos regulatorios del sector

Los resultados de estas auditorías se integran como insumos directos para ajustes del modelo.

22.4 Retroalimentación de Usuarios y Áreas Operativas

El protocolo incorpora observaciones del personal involucrado en el proceso:

Supervisores

Evaluadores H-FRA

RRHH, TI y Seguridad Física

Líderes de área

Se busca detectar puntos de fricción, ambigüedades, duplicidades o necesidades emergentes, permitiendo optimizar la experiencia operativa.

22.5 Entrenamiento y Actualización Continua

Todo el personal involucrado debe recibir capacitación periódica sobre:

Nuevos criterios de riesgo humano

Cambios en el protocolo y herramientas

Nuevos EWI incorporados

Actualizaciones normativas aplicables

La actualización debe registrarse en el historial formativo de cada colaborador.

22.6 Control de Cambios

Cada ajuste del protocolo debe reflejar:

Fecha de modificación

Versión del documento

Motivo del cambio

Responsable de la actualización

Impacto esperado en el proceso

Este control asegura trazabilidad, orden documental y cumplimiento regulatorio.

23. Límites Éticos y Marco Legal

El sistema H-FRA se fundamenta en principios de respeto, proporcionalidad y responsabilidad. Su aplicación debe garantizar la protección de derechos laborales, privacidad y dignidad de las personas, evitando cualquier uso indebido de la información o de sus resultados.

23.1 Principios Éticos del Análisis de Riesgo Humano

El modelo se rige por un marco ético que establece límites claros sobre qué puede y qué no puede evaluarse:

Evaluación basada exclusivamente en conductas y riesgos observables
Se analizan hechos, acciones y patrones operativos, no características personales, estados subjetivos o inferencias psicológicas no verificables.

Minimización y pertinencia de datos
Solo se recopila información estrictamente necesaria para la finalidad de prevención y gestión del riesgo humano.

Prohibición de evaluar atributos protegidos
Quedan excluidos, sin excepción:

creencias religiosas,

preferencias políticas,

orientación sexual,

origen étnico,

afiliación sindical,

datos médicos o condición de salud,
a menos que exista obligación legal explícita.

No discriminación y prohibición de represalias
Ningún resultado H-FRA puede utilizarse para acciones disciplinarias que no estén sustentadas en hechos verificables, políticas internas o normativa laboral vigente.

Proporcionalidad y finalidad legítima
Toda acción debe estar alineada con la protección de activos, seguridad operativa y continuidad del negocio, evitando prácticas excesivas o invasivas.

23.2 Consentimiento y Confidencialidad

La interacción con los colaboradores dentro del sistema H-FRA debe cumplir con protocolos formales de transparencia:

Declaración de propósito en cada entrevista
Antes de iniciar, el evaluador debe comunicar:

objetivo de la entrevista,

alcance del proceso,

almacenamiento y uso de la información,

derechos del colaborador.

Grabación con consentimiento explícito
Cualquier registro audiovisual solo puede iniciarse con consentimiento verbal expresado y documentado. Sin consentimiento, la entrevista debe realizarse sin grabación.

Clasificación documental
Toda la información generada se etiqueta bajo la categoría:
“Confidencial – Riesgo Humano”,
aplicando controles de acceso y resguardo adecuados.

Acceso restringido por rol
Solo el personal autorizado y debidamente acreditado puede consultar información del proceso.

23.3 Protección de Datos

El manejo de datos dentro del modelo debe cumplir con leyes laborales, normas de privacidad y políticas internas vigentes.

Exclusión de datos sensibles prohibidos
No se almacenan ni procesan datos considerados sensibles por normativas de protección de datos, salvo obligación legal.

Anonimización y segmentación de la información
Siempre que sea posible, las bases de datos deben mantener:

minimización de campos personales,

anonimización o pseudonimización de registros,

separación entre datos personales y matrices de análisis.

Retención limitada y eliminación programada
Los documentos se conservan solo el tiempo definido en la política de retención corporativa y luego se eliminan de manera segura.

Trazabilidad de accesos y modificaciones
Todo acceso, descarga o edición debe quedar registrado para auditoría.

24. Protocolo de Escalamiento y Medidas Disciplinarias

El Protocolo de Escalamiento establece los pasos a seguir cuando un caso H-FRA supera niveles de riesgo aceptables. El objetivo es actuar con rapidez, proporcionalidad y fundamento documental, protegiendo tanto a la organización como al colaborador implicado.

24.1 Escalamiento por Puntaje H-FRA

El puntaje integrado del Modelo H-FRA (Probabilidad × Motivación × Acceso × Impacto) determina el nivel de intervención:

Rango	Clasificación	Acciones Requeridas
0–55	Riesgo Bajo	Seguimiento regular; actividades preventivas; revisión trimestral.
56–75	Riesgo Medio	Acciones correctivas obligatorias; actualización del plan de tratamiento; seguimiento mensual.
76–100	Riesgo Alto o Crítico	Activación del Comité de Escalamiento en un plazo de 24–72 horas; medidas de contención inmediatas.

Nota: Cualquier incremento brusco en los Indicadores Tempranos (EWI), aun con puntaje previo bajo, habilita una revisión extraordinaria.

24.2 Acciones Disciplinarias Permitidas

Las acciones disciplinarias deben ser proporcionales al nivel de riesgo, estar alineadas con la política interna y ejecutarse solo cuando existe evidencia verificable.

Revocación temporal de accesos

Aplicable en casos de riesgo técnico o intentos de acceso no autorizados.

Puede incluir privilegios de sistemas, áreas físicas o dispositivos.

Suspensión preventiva

Procede cuando las conductas observadas representan riesgo inmediato.

Debe contar con informe documentado, avalado por Seguridad, RRHH y Legal.

Reubicación temporal

Para casos donde el riesgo está asociado al entorno, funciones o accesos.

Revaluación obligatoria en máximo 30 días.

Terminación laboral

Última instancia.

Solo aplicable cuando el expediente está completo, la conducta infringe políticas críticas o constituye violación grave a normas internas o legales.

Debe ser aprobada por RRHH, Legal y el Comité de Escalamiento.

24.3 Protección del Colaborador

La aplicación del Protocolo H-FRA debe garantizar el respeto a los derechos y la integridad del colaborador. Esto implica:

Evidencia obligatoria
Ninguna acción disciplinaria puede ejecutarse sin:

registros documentales,

hallazgos verificables,

trazabilidad de decisiones.

Validación formal de RRHH y Legal
Toda acción debe ser revisada por ambas áreas antes de su aplicación, sin excepción.

Prohibición de arbitrariedad
Las decisiones deben basarse en conductas, hechos y documentación, nunca en percepciones subjetivas o sesgos.

Comunicación formal del proceso
El colaborador tiene derecho a conocer el motivo de las medidas tomadas y el marco normativo que las respalda.

25. Indicadores de Madurez del Programa H-FRA

El nivel de madurez del Programa H-FRA permite evaluar el grado de desarrollo, integración y sofisticación del sistema de análisis de riesgo humano dentro de la organización. Esta medición facilita definir metas de mejora, asignar recursos y alinear el modelo con estándares internacionales.

Nivel 1: Reactivo

Características principales:

El análisis se realiza únicamente después de incidentes o pérdidas.

No existen herramientas formales de evaluación.

Dependencia total de reportes manuales o denuncias internas.

Casi nula visibilidad sobre patrones de riesgo humano.

Indicadores:

No hay EWI activos.

0 % de cobertura anual.

Documentación fragmentada.

Nivel 2: Básico

Características principales:

Aplicación anual del protocolo para cumplir con requisitos mínimos.

Uso de plantillas y formularios estándar.

Evaluaciones reactivas y parcialmente preventivas.

Capacitación inicial del personal clave.

Indicadores:

Cobertura del 30–50 %.

Registro documental centralizado.

Planes de tratamiento básicos.

Nivel 3: Estructurado

Características principales:

La aplicación del H-FRA se prioriza según criticidad del puesto.

Procesos definidos con roles y responsabilidades formales.

Integración con RRHH, Seguridad Física y TI.

Uso sistemático de EWI técnicos y conductuales.

Indicadores:

Cobertura del 60–80 %.

Revisión semestral del modelo.

Matrices de riesgo integradas y dinamizadas por accesos y funciones.

Nivel 4: Integrado

Características principales:

Automatización parcial del flujo H-FRA.

Sistemas de monitoreo en tiempo real para EWI.

Paneles de control con métricas, alertas y tendencias.

Comité de Escalamiento funcionando de forma preventiva.

Cultura de seguridad en proceso de consolidación.

Indicadores:

Cobertura del 90 % o superior.

Alertas generadas automáticamente.

Reducción documentada de incidentes y falsas alarmas.

Nivel 5: Predictivo

Características principales:

Modelo avanzado con análisis estadístico y proyecciones.

Uso de algoritmos de machine learning sin datos sensibles, respetando completamente la privacidad y el marco ético.

Identificación anticipada de patrones de riesgo.

Integración plena con sistemas corporativos de riesgo y continuidad del negocio.

Indicadores:

Detección temprana con alta precisión.

Curva de incidentes descendente y estable.

Mejora continua basada en análisis multivariable.

26. Riesgos del Sistema H-FRA y Cómo Mitigarlos

La implementación del modelo H-FRA implica riesgos operativos, éticos y procedimentales que deben gestionarse de manera sistemática. Esta sección identifica los principales riesgos inherentes al proceso y define las medidas de mitigación que garantizan la integridad, objetividad y confiabilidad del sistema.

26.1 Sesgos del Evaluador

Riesgo:
El evaluador puede incurrir en sesgos cognitivos (confirmación, atribución, halo, afinidad, prejuicio de autoridad, entre otros), afectando la objetividad del resultado.

Mitigación:

Doble validación obligatoria de todas las evaluaciones (segundo evaluador o supervisor).

Capacitación anual en sesgos cognitivos y evaluación objetiva.

Uso de checklists estandarizados para reducir interpretaciones subjetivas.

Registro transparente y trazable del proceso de evaluación.

26.2 Sobrecorrección Disciplinaria

Riesgo:
Aplicar medidas disciplinarias excesivas, prematuras o no proporcionales al riesgo, generando injusticia organizacional o clima de temor.

Mitigación:

Todas las decisiones deben pasar por un Comité Multidisciplinario (RRHH, Legal, Seguridad).

Obligatoriedad de evidencia verificable antes de cualquier acción.

Matriz de proporcionalidad disciplinaria alineada con políticas internas.

Documentación completa del razonamiento y fundamento legal/operativo de cada medida.

26.3 Clasificación Incorrecta por Falta de Datos

Riesgo:
Evaluaciones incompletas o puntajes mal calculados por ausencia de observación directa o datos insuficientes.

Mitigación:

Observaciones BBS-H obligatorias, en tres momentos diferentes.

Validación cruzada con TI, Seguridad Física y RRHH.

Regla de “no decisión” si los datos no cumplen el estándar mínimo.

Auditoría interna mensual de consistencia en matrices y puntajes.

26.4 Uso Indebido de la Información

Riesgo:
Accesos no autorizados, filtraciones, consultas indebidas o manipulación de información del sistema H-FRA.

Mitigación:

Auditoría trimestral de accesos a la base de datos H-FRA.

Autenticación multifactor y asignación de permisos basada en rol (RBAC).

Trazabilidad completa de accesos, descargas y modificaciones.

Política de sanciones claras ante uso indebido de la información.

Almacenamiento segmentado y cifrado según normativas internas.

27. Anexos Operativos

Los anexos operativos proporcionan herramientas prácticas, estandarizadas y verificables para garantizar que la aplicación del modelo H-FRA sea consistente, auditable y reproducible en toda la organización. Cada anexo complementa una fase operativa del proceso y facilita la labor de los evaluadores y supervisores.

27.1 Guion de Entrevista Semiestructurada

El guion contiene preguntas abiertas y de confirmación organizadas en 12 dimensiones clave, orientadas a identificar factores de riesgo sin invadir la privacidad ni evaluar variables protegidas. Las dimensiones incluyen:

Percepción de justicia organizacional

Carga emocional y estrés percibido

Fatiga física o mental

Lealtad y compromiso con la misión organizacional

Expectativas laborales (rol, crecimiento, reconocimiento)

Clima laboral y relaciones interpersonales

Cambios recientes en el entorno de trabajo

Disponibilidad de recursos y soporte

Percepción de seguridad física y digital

Cumplimiento de normas y protocolos

Sentido de autoeficacia y control sobre el trabajo

Identificación de conductas observables críticas

Incluye instrucciones para:

apertura ética de la entrevista,

manejo de silencios,

preguntas de seguimiento sin sesgo,

cierre y documentación.

27.2 Diccionario de Desviaciones Conductuales

Este documento define y estandariza los criterios utilizados en la observación BBS-H, para evitar discrepancias entre evaluadores.

Incluye definiciones claras de:

Desviación leve:
Incumplimiento menor que no genera riesgo inmediato ni intencionalidad, pero requiere corrección.

Desviación crítica:
Conducta que compromete la seguridad, los activos o la información; implica omisión grave, violación deliberada o riesgo inminente.

El diccionario proporciona ejemplos por categoría (accesos, documentos, dispositivos, comportamiento físico, cumplimiento de políticas).

27.3 Procedimiento de Observación BBS-H

Guía paso a paso para supervisores y evaluadores, que garantiza homogeneidad en la observación de comportamientos.

Incluye:

Preparación previa y revisión de criterios.

Observación directa en tres momentos distintos.

Registro inmediato en formato oficial.

Validación cruzada con actores relevantes.

Clasificación en correcto, desviación leve o crítica.

Reglas de neutralidad (no intervenir salvo riesgo real).

Lineamientos para retroalimentación al colaborador.

También incorpora una lista de chequeo y ejemplos de buenas y malas prácticas.

27.4 Plantilla de Cálculo del H-FRA Score

Herramienta oficial para garantizar la trazabilidad y coherencia del puntaje integrado.

Incluye:

Campos para Probabilidad, Motivación, Acceso y Impacto.

Instrucciones para ponderación y normalización.

Validación automática de incoherencias (p. ej., puntajes fuera de rango o sin datos suficientes).

Espacios para justificación objetiva del evaluador.

Registro de doble validación según la política anti-sesgo.

Indicador automático de nivel de riesgo (bajo, medio, alto/crítico).

Puede ser utilizado en formato digital o impreso para auditorías internas.

28. Glosario

A continuación, se presentan las definiciones estandarizadas de los conceptos clave utilizados en este documento:

Riesgo humano: Posibilidad de que una persona, por acción u omisión, genere incidentes o pérdidas para la organización.

Insider: Individuo con acceso autorizado a información, sistemas o instalaciones, que podría aprovechar dicho acceso de manera indebida.

Desviación: Conducta que se aparta de los procedimientos, normas o expectativas establecidas.

Acceso privilegiado: Permisos o facultades que otorgan a una persona la capacidad de realizar acciones sensibles o críticas dentro de la organización.

Perfil crítico: Función, puesto o persona cuya actividad involucra riesgos significativos para la seguridad o la operación.

Fatiga: Estado físico o mental que reduce la capacidad de una persona para desempeñar correctamente sus tareas y aumenta la probabilidad de error.

Conducta sospechosa: Acciones o comportamientos que, por su naturaleza o contexto, podrían indicar intenciones fuera de lo permitido o esperado.

Violación intencional: Incumplimiento deliberado de normas, políticas o procedimientos.

Error humano: Acción involuntaria que genera un resultado no deseado o diferente al esperado.

29. Referencias y Bibliografía

El presente protocolo se fundamenta en metodologías internacionalmente reconocidas en materia de análisis de riesgo humano, seguridad corporativa, ergonomía, psicología organizacional y prevención de amenazas internas. Las siguientes fuentes constituyen el marco teórico–técnico principal del modelo H-FRA:

Normas, Estándares y Guías Internacionales

FAA – Human Factors Analysis and Classification System (HFACS), 2023 Update.
Marco base para la clasificación de fallas humanas y la identificación de factores latentes.

ISO 31030:2021 – Traveller Security.
Lineamientos aplicables a gestión de riesgos, seguridad del personal y protección de activos.

ISO 31000 – Risk Management Guidelines.
Referente global para la estructuración de procesos formales de gestión de riesgo.

ISO 45001 – Occupational Health & Safety Management Systems.
Orientación para el análisis de factores humanos y condiciones de trabajo.

NIST Special Publication 800-53 Revision 5 – Security and Privacy Controls.
Fuente principal para controles de amenazas internas, accesos y monitoreo.

NIST Insider Threat Guide.
Enfoque específico sobre riesgo interno, perfiles y controles compensatorios.

Manuales y Modelos Especializados

DOE (Department of Energy) – Human Reliability Analysis Handbook.
Base para THERP, HEART y métodos cuantitativos de probabilidad de error humano.

HEART – Human Error Assessment and Reduction Technique.
Modelo para evaluación rápida de probabilidad de error en tareas críticas.

THERP – Technique for Human Error Rate Prediction.
Referencia para análisis probabilístico de fallas humanas por tarea.

Behavior-Based Safety (BBS) Literature – Varias fuentes académicas.
Modelos de observación conductual en seguridad industrial y análisis de hábitos de riesgo.

ILO PRIMA – Psychosocial Risk Management Approach, 2022 Edition.
Base internacional para el análisis de factores psicosociales y estrés laboral.

Otras Fuentes Especializadas

Publicaciones de seguridad corporativa sobre insider threat, fraude interno y análisis conductual.

Estudios de psicología organizacional relacionados con clima laboral, carga emocional y desempeño humano.

Documentos de auditoría y compliance corporativo para alineación con buenas prácticas globales.